

Completely normal elements in finite abelian extensions

JA KYUNG KOO AND DONG HWA SHIN

Abstract

We give a completely normal element in the maximal real subfield of a cyclotomic field over the field of rational numbers, which is different from [13]. This result is a consequence of the criterion for a normal element developed in [7]. Furthermore, we find a completely normal element in certain extension of modular function fields in terms of a quotient of the modular discriminant function.

1 Introduction

Let L/K be a finite Galois extension. By the normal basis theorem [14] there exists an element $x \in L$ such that $\{x^\gamma \mid \gamma \in \text{Gal}(L/K)\}$ is a K -basis of L , a so-called *normal basis* of L/K . Such an element x is said to be *normal* in L/K . Moreover, if x is normal in L/F for every intermediate field F , then x is said to be *completely normal* in L/K . The existence of a completely normal element was first proved by Blessenohl and Johnsen [1].

Throughout this paper we let $\zeta_\ell = e^{2\pi i/\ell}$ be a primitive ℓ th root of unity for a positive integer ℓ . Furthermore, we let $\mathbb{Q}(\zeta_\ell)^+$ be the maximal real subfield of the ℓ th cyclotomic field $\mathbb{Q}(\zeta_\ell)$.

Okada [13] proved that if k and ℓ (> 2) are positive integers with k odd and T is a set of representatives for which $(\mathbb{Z}/\ell\mathbb{Z})^\times = T \cup (-T)$, then the numbers $(1/\pi^k)(d/dz)^k(\cot \pi z)|_{z=a/\ell}$ for $a \in T$ form a normal basis of $\mathbb{Q}(\zeta_\ell)^+/\mathbb{Q}$, which generalized the works of Chowla [2] when $k = 1$. He utilized the partial fractional decomposition of $(d/dz)^k(\cot \pi z)$ and the Frobenius determinant relation [11, Chapter 21 Theorem 5].

2010 *Mathematics Subject Classification.* 11F03, 11R18, 12F05.

Key words and phrases. cyclotomic extensions, modular functions, normal bases.

This research was partially supported by Basic Science Research Program through the NRF of Korea funded by MEST (2011-0001184). The second named author was partially supported by TJ Park Postdoctoral Fellowship.

On the other hand, let \mathcal{N} be the set of positive integers which are either odd or divisible by 4. Let $\ell \in \mathcal{N}$. Hachenberger [5] constructed an element $w \in \mathbb{Q}(\zeta_\ell)$ which is simultaneously normal in $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_n)$ for each $n \in \mathcal{N}$ dividing ℓ . The main tool is the notion of cyclic submodules in $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_n)$ [4].

Let K be an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. For an integer ℓ (≥ 2) let $K_{(\ell)}$ be the ray class field of K modulo ℓ . Recently, Jung et al [7] showed that the singular value of a Siegel function is normal in $K_{(\ell)}/K$. To this end, they derived a criterion to determine a normal element in a finite abelian extension of number fields from the Frobenius determinant relation.

Actually the criterion can be extended to determine a completely normal element in a finite abelian extension (Theorem 2.2). In this paper we shall give a completely normal element in $\mathbb{Q}(\zeta_\ell)^+/\mathbb{Q}$ for an integer ℓ (≥ 5) by using the criterion (Theorems 3.1 and 3.2). The element is expressed in terms of the cosine function, which is simple and totally different from that of [13]. Furthermore, we shall find a completely normal element in certain extension of modular function fields in terms of a quotient of the modular discriminant function (Theorem 4.3).

2 A criterion for completely normal elements

Throughout this section we let L/K be a finite abelian extension of degree n (≥ 2) with $G = \text{Gal}(L/K)$. Furthermore, we let $|\cdot|$ be a valuation on L . Then $|\cdot|$ satisfies the triangle inequality, namely, $|x + y| \leq |x| + |y|$ for all $x, y \in L$. It follows that

$$(1) \quad |x| - |y| \leq |x + y| \quad \text{for all } x, y \in L.$$

In particular, if $|\cdot|$ is nonarchimedean, then $|x + y| \leq \max\{|x|, |y|\}$, from which one can readily deduce that

$$(2) \quad |x|^m - |y|^m \leq |x + y|^m \quad \text{for all } x, y \in L \text{ and any positive real number } m$$

[6, Chapter II §1].

LEMMA 2.1. *An element $x \in L$ is normal in L/K if and only if*

$$\sum_{\gamma \in G} \chi(\gamma^{-1}) x^\gamma \neq 0 \quad \text{for all characters } \chi \text{ on } G.$$

PROOF. [7, Proposition 2.3]. □

THEOREM 2.2. *Assume that there exists an element $x \in L$ such that*

$$|x^\gamma/x| < 1 \quad \text{for all } \gamma \in G - \{\text{Id}\}.$$

Let m be any positive integer such that

$$(3) \quad |x^\gamma/x|^m \leq 1/n \quad \text{for all } \gamma \in G - \{\text{Id}\}.$$

Then x^m is completely normal in L/K . In particular, if $|\cdot|$ is nonarchimedean, then any positive power of x is completely normal in L/K .

PROOF. Let F be an intermediate field of L/K with $\ell = [L : F]$ and $H = \text{Gal}(L/F)$ ($\leq G$). For any character χ on H we find that

$$\begin{aligned} \left| \sum_{\gamma \in H} \chi(\gamma^{-1})(x^m)^\gamma \right| &\geq |x^m| \left(1 - \sum_{\gamma \in H - \{\text{Id}\}} |(x^m)^\gamma/x^m| \right) \quad \text{by (1)} \\ &\geq |x^m| (1 - (1/n)(\ell - 1)) \quad \text{by (3)} \\ &= |x^m| (n - \ell + 1)/n \\ &> 0 \quad \text{because } \ell \leq n. \end{aligned}$$

This shows that x^m is normal in L/F by Lemma 2.1; and hence x^m is completely normal in L/K . Furthermore, if $|\cdot|$ is nonarchimedean, then we derive for any positive integer t that

$$\begin{aligned} \left| \sum_{\gamma \in H} \chi(\gamma^{-1})(x^t)^\gamma \right|^m &\geq |x^t|^m \left(1 - \sum_{\gamma \in H - \{\text{Id}\}} |(x^t)^\gamma/x^t|^m \right) \quad \text{by (2)} \\ &\geq |x^t|^m (1 - (1/n)^t(\ell - 1)) \quad \text{by (3)} \\ &\geq |x^t|^m (1 - (1/n)(\ell - 1)) \\ &= |x^t|^m (n - \ell + 1)/n \\ &> 0 \quad \text{because } \ell \leq n. \end{aligned}$$

Hence x^t is completely normal in L/K again by Lemma 2.1. This completes the proof. \square

COROLLARY 2.3. Let L/K be an abelian extension of number fields. Assume that there exists an element $x \in L$ such that

- (i) x is an algebraic integer,
- (ii) $L = K(x)$,
- (iii) x^γ are real for all $\gamma \in G$.

Let a and b be nonzero integers such that $2 < |a/b|$, where $|\cdot|$ is the usual absolute value on \mathbb{C} . Then, a high power of $ax + b$ is completely normal in L/K .

PROOF. Suppose that there exist distinct elements γ and δ of G such that $|ax^\gamma + b| = |ax^\delta + b|$. Since x^γ and x^δ are real by the assumption (iii), we get $ax^\gamma + b = \pm(ax^\delta + b)$. Moreover, since $x^\gamma \neq x^\delta$ by the assumption (ii) and the fact $\gamma \neq \delta$, we obtain $ax^\gamma + b = -(ax^\delta + b)$, from which it follows that $x^\gamma + x^\delta = -2b/a$. Note that $x^\gamma + x^\delta$ is an algebraic integer by the assumption (i), but $-2b/a$ is a rational number such that $0 < |2b/a| < 1$, which yields a contradiction.

For each intermediate field F of L/K with $[L : F] \geq 2$, the preceding argument shows that there is a unique element γ_F of $\text{Gal}(L/F)$ and a positive integer m_F such that $|(ax^\gamma + b)/(ax^{\gamma_F} + b)|^{m_F} \leq 1/[L : F]$ for all $\gamma \in \text{Gal}(L/F) - \{\gamma_F\}$. If we set $m = \max\{m_F | F\}$, then we get from Theorem 2.2 that $(ax^{\gamma_F} + b)^m$ is completely normal in L/F . In particular, the set $\{((ax^{\gamma_F} + b)^m)^\gamma | \gamma \in \text{Gal}(L/F)\}$ is a normal basis of L over F ; and hence $((ax^{\gamma_F} + b)^m)^{\gamma_F^{-1}} = (ax + b)^m$ is normal in L/F . This implies that $(ax + b)^m$ is completely normal in L/K because F is arbitrary. This completes the proof. \square

REMARK 2.4. If L/K is an abelian extension of totally real number fields, then there always exists such an element $x \in L$ which satisfies the assumptions of Corollary 2.3.

3 Maximal real subfields of cyclotomic fields

Let ℓ be a positive integer. As is well-known, $\mathbb{Q}(\zeta_\ell)^+ = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ and $\text{Gal}(\mathbb{Q}(\zeta_\ell)^+/\mathbb{Q}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times / \{\pm 1\}$, whose actions are given as follows: if $t \in (\mathbb{Z}/\ell\mathbb{Z})^\times / \{\pm 1\}$, then $(\zeta_\ell + \zeta_\ell^{-1})^t = \zeta_\ell^t + \zeta_\ell^{-t}$. Denote the number of positive integers relatively prime to ℓ by $\phi(\ell)$. Then we have

$$[\mathbb{Q}(\zeta_\ell)^+ : \mathbb{Q}] = \begin{cases} 1, & \text{if } \ell = 1, 2, 3, 4, 6, \\ \phi(\ell)/2 (\geq 2), & \text{otherwise} \end{cases}$$

[15, Chapter 2].

Let $|\cdot|$ denote the usual absolute value on \mathbb{C} .

THEOREM 3.1. *Let ℓ ($\neq 1, 2, 3, 4, 6$) be a positive integer. If m is any positive integer such that*

$$((\cos(4\pi/\ell) + 1)/(\cos(2\pi/\ell) + 1))^m \leq 2/\phi(\ell),$$

then $(\cos(2\pi/\ell) + 1)^m$ is completely normal in $\mathbb{Q}(\zeta_\ell)^+/\mathbb{Q}$.

PROOF. Let $x = (\zeta_\ell + \zeta_\ell^{-1})/2 + 1 = \cos(2\pi/\ell) + 1$. If $\gamma \in \text{Gal}(\mathbb{Q}(\zeta_\ell)^+/\mathbb{Q}) - \{\text{Id}\}$, then $x^\gamma = (\zeta_\ell^t + \zeta_\ell^{-t})/2 + 1$ for some integer t with $\gcd(\ell, t) = 1$ and $1 < t \leq [\ell/2]$, where $[\cdot]$ is the Gauss symbol. We achieve that

$$\begin{aligned} |x^\gamma/x| &= |((\zeta_\ell^t + \zeta_\ell^{-t})/2 + 1)/((\zeta_\ell + \zeta_\ell^{-1})/2 + 1)| \\ &= |(\cos(2t\pi/\ell) + 1)/(\cos(2\pi/\ell) + 1)| \\ &\leq |(\cos(4\pi/\ell) + 1)/(\cos(2\pi/\ell) + 1)|, \end{aligned}$$

which is less than 1. The result follows from Theorem 2.2. \square

THEOREM 3.2. *Let ℓ (≥ 5) be an odd integer. If m is any positive integer such that*

$$(\cos(2\pi/\ell)/\cos(\pi/\ell))^m \leq 2/\phi(\ell),$$

then $\cos^m(\pi/\ell)$ is completely normal in $\mathbb{Q}(\zeta_\ell)^+/\mathbb{Q}$.

PROOF. Let $x = -(\zeta^{(\ell-1)/2} + \zeta^{-(\ell-1)/2})/2$. Since $1 \cdot \ell + (-2) \cdot (\ell-1)/2 = 1$, we get $\gcd(\ell, (\ell-1)/2) = 1$, which implies that x is a conjugate of $-(\zeta + \zeta^{-1})/2$. Hence, if $\gamma \in \text{Gal}(\mathbb{Q}(\zeta_\ell)^+/\mathbb{Q}) - \{\text{Id}\}$, then $x^\gamma = -(\zeta^t + \zeta^{-t})/2$ for some integer t with $\gcd(\ell, t) = 1$ and $1 \leq t < (\ell-1)/2$. We find that

$$\begin{aligned} |x^\gamma/x| &= |(-(\zeta^t + \zeta^{-t})/2)/(-(\zeta^{(\ell-1)/2} + \zeta^{-(\ell-1)/2})/2)| \\ &= |-\cos(2t\pi/\ell)/-\cos(\pi - \pi/\ell)| \\ &= |\cos(2t\pi/\ell)|/\cos(\pi/\ell) \\ &\leq \cos(2\pi/\ell)/\cos(\pi/\ell), \end{aligned}$$

which is less than 1. We obtain the assertion by Theorem 2.2. \square

LEMMA 3.3. *Let L_1 and L_2 be finite Galois extensions of a number field K such that $L_1 \cap L_2 = K$. If $x_k \in L_k$ is normal in L_k/K ($k = 1, 2$), then x_1x_2 is normal in L_1L_2/K .*

PROOF. [8, p.227]. \square

LEMMA 3.4. *Let $t = 4$ or an odd prime p such that $p \equiv 3 \pmod{4}$. Then $\mathbb{Q}(\zeta_t)$ contains a unique quadratic extension of \mathbb{Q} , namely $\mathbb{Q}(\sqrt{-t})$.*

PROOF. [6, Theorem 11.1]. \square

THEOREM 3.5. *Let $t = 4$ or an odd prime p such that $p \equiv 3 \pmod{4}$. Let ℓ ($\neq 1, 2, 3, 4, 6$) be a positive integer. If m is any positive integer such that*

$$(4) \quad ((\cos(4\pi/t\ell) + 1)/(\cos(2\pi/t\ell) + 1))^m \leq 2/\phi(t\ell),$$

then $(\sqrt{-t} + 1)(\cos(2\pi/t\ell) + 1)^m$ is normal in $\mathbb{Q}(\zeta_{t\ell})/\mathbb{Q}$.

PROOF. One can readily show that $\sqrt{-t} + 1$ is normal in $\mathbb{Q}(\sqrt{-t})/\mathbb{Q}$. And, if m is any positive integer which satisfies the condition (4), then $(\cos(2\pi/t\ell) + 1)^m$ is normal in $\mathbb{Q}(\zeta_{t\ell})^+/\mathbb{Q}$ by Theorem 3.1. On the other hand, since $\mathbb{Q}(\sqrt{-t})$ is an imaginary quadratic field contained in $\mathbb{Q}(\zeta_t)$ ($\subset \mathbb{Q}(\zeta_{t\ell})$) by Lemma 3.4, we have $\mathbb{Q}(\sqrt{-t}) \cap \mathbb{Q}(\zeta_{t\ell})^+ = \mathbb{Q}$ and $\mathbb{Q}(\sqrt{-t})\mathbb{Q}(\zeta_{t\ell})^+ = \mathbb{Q}(\zeta_{t\ell})$. Now, the result follows from Lemma 3.3. \square

4 Fields of modular functions

Let $\mathbb{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$ be the complex upper half-plane. For a positive integer N we consider the group

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\},$$

which acts on $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ as fractional linear transformations. Then a (meromorphic) *modular function* for $\Gamma_0(m)$ is a \mathbb{C} -valued function on \mathbb{H} , except for isolated singularities, which satisfies the following three conditions:

- (i) $f(\tau)$ is meromorphic on \mathbb{H} ,
- (ii) $f(\tau)$ is invariant under $\Gamma_0(N)$,
- (iii) $f(\tau)$ is meromorphic at the cusps $\mathbb{Q} \cup \{\infty\}$

[3, §11 B]. We denote the field of all modular functions for $\Gamma_0(N)$ by $\mathbb{C}(X_0(N))$. As is well-known, $\mathbb{C}(X_0(N))$ is a Galois extension of $\mathbb{C}(X_0(1))$ whose Galois group is isomorphic to the quotient group $\Gamma_0(1)/\Gamma_0(N)$ [11, Chapter 6].

For a pair $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$, the *Siegel function* $g_{(r_1, r_2)}(\tau)$ on \mathbb{H} is defined by the following infinite product

$$g_{(r_1, r_2)}(\tau) = -q^{(1/2)\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)} (1 - q^{r_1} e^{2\pi i r_2}) \prod_{n=1}^{\infty} (1 - q^{n+r_1} e^{2\pi i r_2}) (1 - q^{n-r_1} e^{-2\pi i r_2}),$$

where $q = e^{2\pi i \tau}$ and $\mathbf{B}_2(X) = X^2 - X + 1/6$ is the second Bernoulli polynomial.

For $X \in \mathbb{R}$ we let $\langle X \rangle$ be the fractional part of X in the interval $[0, 1)$.

LEMMA 4.1. *Let $N (\geq 2)$ be an integer and $(r_1, r_2) \in (1/N)\mathbb{Z}^2 - \mathbb{Z}^2$.*

- (i) $g_{(r_1, r_2)}(\tau)^{12N}$ is determined by $\pm(r_1, r_2) \pmod{\mathbb{Z}^2}$.
- (ii) If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$, then

$$g_{(r_1, r_2)}(\tau)^{12N} \circ \alpha = g_{(r_1, r_2)\alpha}(\tau)^{12N} = g_{(r_1 a + r_2 c, r_1 b + r_2 d)}(\tau)^{12N}.$$

- (iii) $\text{ord}_q g_{(r_1, r_2)}(\tau) = (1/2)\mathbf{B}_2(\langle r_1 \rangle)$.

PROOF. [10, Chapter 2 §1]. □

Let

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24} \quad (\tau \in \mathbb{H})$$

be the *modular discriminant function*.

LEMMA 4.2. *We have the relation*

$$\Delta(\tau)/\Delta(N\tau) = N^{12} \prod_{k=1}^N g_{(0,k/N)}(\tau)^{-12},$$

which is a modular function for $\Gamma_0(N)$.

PROOF. [9, Proposition 5.1]. □

THEOREM 4.3. *Let $N (\geq 2)$ be an integer. Let $L = \mathbb{C}(X_0(N))$ and K be the subfield of L fixed by $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ in $\Gamma_0(1)/\Gamma_0(N)$. Then, any positive power of $\Delta(\tau)/\Delta(N\tau)$ is completely normal in L/K .*

PROOF. By Galois theory we have

$$\begin{aligned} \text{Gal}(L/K) &\simeq \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \text{ in } \Gamma_0(1)/\Gamma_0(N) \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \mid t = 0, 1, \dots, N-1 \right\} \text{ in } \Gamma_0(1)/\Gamma_0(N). \end{aligned}$$

Consider the nonarchimedean valuation $|\cdot|$ on L defined by

$$\begin{aligned} |\cdot| : L &\longrightarrow \mathbb{R}_{\geq 0} \\ \alpha &\mapsto |\alpha| = \exp(-\text{ord}_q \alpha). \end{aligned}$$

Let $x = \Delta(\tau)/\Delta(N\tau)$. For any $\gamma = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \in \text{Gal}(L/K) - \{\text{Id}\}$ we find that

$$\begin{aligned} |x^\gamma/x|^N &= \left| (N^{12N} \prod_{k=1}^{N-1} g_{(0,k/N)}(\tau)^{-12N})^\gamma / N^{12N} \prod_{k=1}^{N-1} g_{(0,k/N)}(\tau)^{-12N} \right| \text{ by Lemma 4.2} \\ &= \left| \prod_{k=1}^{N-1} g_{(kt/N, k/N)}(\tau)^{-12N} / \prod_{k=1}^{N-1} g_{(0,k/N)}(\tau)^{-12N} \right| \text{ by Lemma 4.1(i) and (ii)} \\ &= \exp \left(- \sum_{k=1}^{N-1} (1/2) \mathbf{B}_2(\langle kt/N \rangle) \cdot (-12N) + \sum_{k=1}^{N-1} (1/2) \mathbf{B}_2(0) \cdot (-12N) \right) \\ &\quad \text{by Lemma 4.1(iii)} \\ &= \exp \left(6N \sum_{k=1}^{N-1} (\mathbf{B}_2(\langle kt/N \rangle) - \mathbf{B}_2(0)) \right) \\ &< 1 \text{ because } \mathbf{B}_2(X) \text{ has its maximum at } X = 0 \text{ in the interval } [0, 1), \end{aligned}$$

from which it follows that $|x^\gamma/x| < 1$. Therefore x is completely normal in L/K by Theorem 2.2. □

References

- [1] D. Blessenohl and K. Johnsen, *Eine Verschärfung des Satzes von der Normalbasis*, J. Algebra 103 (1986), 141–159.
- [2] S. Chowla, *The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation*, J. Number Theory 2 (1970), 120–123.
- [3] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., 1989.
- [4] D. Hachenberger, *Finite Fields: Normal Bases and Completely Free Elements*, Kluwer, Boston, 1997.
- [5] D. Hachenberger, *Universal normal bases for the abelian closure of the field of rational numbers*, Acta Arith. 93 (2000), no. 4, 329–341.
- [6] G. J. Janusz, *Algebraic Number Fields*, 2nd ed., Amer. Math. Soc., 1996.
- [7] H. Y. Jung, J. K. Koo and D. H. Shin, *Normal bases of ray class fields over imaginary quadratic fields*, Math. Zeit., to appear.
- [8] F. Kawamoto, *On normal integral bases*, Tokyo J. Math. 7 (1984), 221–231.
- [9] J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit., 264 (2010) 137–177.
- [10] D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Springer-Verlag, 1981.
- [11] S. Lang, *Elliptic Functions*, 2nd ed., Springer-Verlag, New York, 1987.
- [12] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.
- [13] T. Okada, *On an extension of a theorem of S. Chowla*, Acta Arith. 38 (1980/81), no. 4, 341–345.
- [14] B. L. van der Waerden, *Algebra, Vol I*, Springer-Verlag, 2003.
- [15] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

DEPARTMENT OF MATHEMATICAL SCIENCES
KAIST

DAEJEON 373-1

KOREA 305-701

E-mail address: jkkoo@math.kaist.ac.kr

DEPARTMENT OF MATHEMATICS AND STATIS-
TICS

MCGILL UNIVERSITY

805 SHERBROOKE ST. WEST

MONTREAL, QUEBEC

CANADA H3A 2K6

E-mail address: dong.hwa.shin@mail.mcgill.ca